立法會
Legislative Council

LC Paper No. CB(4)826/13-14(06)

Ref. : CB4/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 22 July 2014

Updated background brief on information security

Purpose

This paper gives a summary of views and concerns raised by Members during previous discussions on the Government's information security programmes.

Background

2. The objectives of the Government's information security programmes are to formulate and implement information security policies and guidelines for compliance and reference by bureaux and departments ("B/Ds"), ensure that all the Government's information technology ("IT") infrastructure, systems and information are secure and resilient, and promote and enhance the awareness of information security and cyber risks among organizations and members of the public in the following three main areas:

(a) information security threats and risks;

(b) information security measures in the Government; and

(c) information security in the wider community.

Summary of views and concerns raised by Members

Information security threats and risks

3. At the meeting of the Panel on Information Technology and Broadcasting ("the Panel") on 8 July 2013, members expressed great concern about media reports relating to Edward Snowden, former analyst of the United States ("US") National Security Agency, which alleged that the local computer systems, including the Hong Kong Internet Exchange ("HKIX") of the Chinese University of Hong Kong, had been hacked by the US Government. Members urged the Administration to take follow-up actions to strengthen information security and data protection.

4. According to the Administration, the HKIX had checked its system setup, and found neither signs of irregular network traffic nor traces of hacking. The Administration assured members that the network security and network traffic of HKIX had all along been closely monitored by designated personnel around the clock and the system had undergone security audit review.

Information security in the Government and wider community

5. At the Panel meeting on 8 July 2013, members expressed doubts as to whether the Government was able to detect and prevent intrusions into its computer systems by professional hackers. They enquired about measures taken to protect against future security attacks on the Government's computer systems. According to the Administration, no incident of hacking leading to leakage of information from the Government computer systems was reported in the past five years. The Administration reassured members that it had adopted on-going security best practices to strengthen its security protection capabilities, including regular security risk assessment and third-party audit for critical IT systems.

6. Some members were of the view that the Administration should step up effort in promoting security awareness and capabilities among local enterprises and the community. As such, they urged the Administration to provide funding support to Hong Kong Computer Emergency Response Team ("HKCERT") which was set up to provide advice on preventive measures against security threats and promote information security awareness. The Administration advised that the annual expenditure in connection with the HKCERT during the past few years were around $7.3 million, and increased to $9.89 million in 2012 and $9.95 million in 2013. The amount of funding was proposed by Hong Kong Productivity Council ("HKPC") each year.

Finance Committee

7. At the special meeting of the Finance Committee on 2 April 2014, Dr Hon Elizabeth QUAT sought information on the financial resources and manpower involved to enhance cyber security and the cooperation with relevant organizations in the community to mitigate cyber risks. According to the Administration, there was an IT security team comprised of nine Office of the Government Chief Information Officer ("OGCIO") staff responsible for handling and coordinating the overall information security activities within the Government, and coordinating information security awareness and education activities for both the Government and the community. The annual expenditure was about $6.05 million. B/Ds would deploy their staff resources to handle their internal IT security matters. In 2014-2015, OGCIO would collaborate with HKCERT to provide services on computer security incident responses, issue security threat alerts and organize education activities for local enterprises, public organizations and the general public, by providing a funding support of about $10 million to the HKPC for delivering the services. OGCIO had also earmarked about $3 million to strengthen the educational activities on information and network security for enterprises and the general public.

Council meetings

8. At the Council meeting on 19 June 2013, Hon Andrew LEUNG, in his capacity as Chairman of the House Committee, moved an adjournment motion under Rule (16)4 of the Rules of Procedures for the purpose of discussing cyber security.

9. At the Council meetings on 7 and 21 May 2014, Hon Charles Peter MOK and Dr Hon Elizabeth QUAT raised questions on the remedial measures to tackle a security loophole found in version 1.0.1 of OpenSSL which was a data encryption technology widely used in electronic network systems. According to the Administration, there were around 90 Government application systems that used OpenSSL version 1.0.1 encryption technology, of which 85 were Government internal applications, while the remaining five were systems that provided electronic services to the public. In view that hackers might make use of the loophole to steal encrypted information in web sites servers and crack other network security measures, the concerned B/Ds had immediately taken appropriate security measures for the affected application systems including installing patches, arranging the renewal of digital certificates and cryptographic keys, and reminding users to change their passwords when necessary. OGCIO had requested all B/Ds to conduct a risk assessment on the affected systems and take remedial actions. Besides, HKCERT and the Hong

Kong Police Force had notified relevant stakeholders by emails on the vulnerabilities of the security loophole, its impacts and responsive measures. This security incident had not affected any Government services.

Latest position

10. The Administration will brief the Panel on 22 July 2014 on the progress and development of the Government's information security programmes.

Relevant papers

11. A list of the relevant papers with their hyperlinks is at:

http://www.legco.gov.hk/yr15-16/english/panels/itb/papers/itb_fs.htm

http://www.legco.gov.hk/yr13-14/english/fc/fc/w_q/cedb-ct-e.pdf

http://www.legco.gov.hk/yr13-14/english/counmtg/question/ques1314.htm#toptbl

Council Business Division 4
Legislative Council Secretariat
22 July 2014